

ABSTRACT OF THE DISCLOSURE

Two embodiments of a method and system to maintain application data secure and authentication token for use therein are provided. The present invention uses transient authentication, in which a small hardware token
5 continuously authenticates the user's presence over a short-range, wireless link. Four principles underlying transient authentication are described as well as the two embodiments for securing applications. In the first embodiment, applications are protected transparently by encrypting in-memory state when the user departs and decrypting this state when the user returns. This technique is effective, requiring
10 just seconds to protect and restore an entire machine. In the second embodiment, applications utilize an API for transient authentication, protecting only sensitive state. Ports of three applications, PGP, SSH, and Mozilla are described with respect to this API.